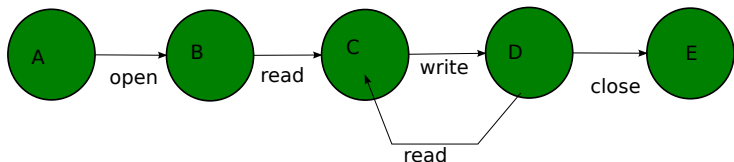


Prior Art: Finite Automata

- Maintain current “state” associated with the syscalls so far (and other info)
- Define transitions between the various states
- When the appropriate syscall is seen, transition to the appropriate new state:



- If an unfamiliar syscall is made, alert